Chapter 12
Hard Clues in Soft Environments:
The Cloud's Influence on Digital Forensics

Andrea Atzeni
Politecnico di Torino, Italy

Paolo Smiraglia
Politecnico di Torino, Italy

Andrea Siringo
Former Student at Politecnico di Torino, Italy

ABSTRACT

Cloud forensics is an open and important area of research due to the growing interest in cloud technology. The increasing frequency of digital investigations brings with it the need for studying specific scenarios in the area of forensics, both when evidence are inside the cloud and when the cloud can be used as platform to perform the investigations. In this chapter we highlight the problems digital forensics must deal with in the Cloud. We introduce historical roots of digital forensics, as well as an overall background about the Cloud and we provide possible meanings of cloud forensics, based on available definitions. Since the cloud introduces different architectural paradigm that affects all the phases of a forensics investigation, in this survey we detail many security issues digital forensics have to face in a cloud environment. We describe when and what available solutions exist and, on the contrary, the still open problems, and we discuss possible future directions in this field.

INTRODUCTION

Cloud computing is of great interest to private and government organizations, always looking for ways to get fast and effective results and to lower the production costs. The Cloud model may enable low costs for accessing computational and storage resources. Due to the implementation of the pay-on-demand model, the economic costs of cloud resources are strictly related to their real usage. Moreover, cloud resources are managed through a web browser, so access and configuration are easy.

DOI: 10.4018/978-1-4666-8387-7.ch012

Given these encouraging premises, market predictions foresee an annual increase for the Cloud of 23.5% in 2013-2016 (from International Data Corporation (IDC) (Gens & Shirer, 2013) and similar by Gartner (Columbus, 2013)). According to other survey results (KPMG International, 2013), half of the companies who currently do not use cloud-based services expressed the intention to adopt them by 2015.

However, despite the will to adopt cloud-based solutions, the same survey highlights that many companies are still worried about security and reliability concerns. These include, for example, data loss and theft of intellectual properties, violation of user privacy, law and regulations compliance and any security risk that may cause service interruption.

As real cases demonstrate, cloud architectures may be involved in both ends of cyber-attacks. For instance, as reported by C. Metz (Metz, 2009), in 2009 Amazon was the victim of a DDoS attack while in 2011 the Amazon cloud was used to breach the PlayStation Network (Galante, Kharif, & Alpeyev, 2011). So the characteristic of flexibility, which is distinctive of the cloud and a source of benefits for companies, can also be exploited to facilitate illicit acts and distribute illegal material. Moreover, in case of attack the volatile nature of cloud provisioned resources may make possible subsequent investigations difficult. So, security solutions need to be specifically developed or adapted for the cloud domain.

In case of a security breach, it is necessary to perform an investigation to clarify who carried out the attack and how the system was infringed. Here the digital forensics practices which have been developed in recent decades come into play. This discipline was born to assist the police in managing the use of electronic devices in criminal acts. It takes care to obtain evidence from any device capable of storing, such as a computer, a smartphone or even a digital camera.

Effectively, digital forensics is the set of best practices used to ensure that the digital evidence extracted from the devices is unaltered. To avoid contamination and subsequent loss of integrity and/or of authenticity, appropriate methods and tools must be adopted at all stages of evidence processing, from seizure of the devices on which the data is stored to the presentation of the results of the analysis performed on the data.

In this chapter we will discuss possible solutions which can be implemented to solve problems arising when an investigation needs to cope with cloud computing architectures. For the sake of clarity, we will introduce concepts and methods of digital forensic followed by distinctive features of cloud computing. Then we will discuss problems deriving by the use of digital forensics in the cloud. Finally, we will detail solutions for some of the technical problems, concluding with open issues and future directions.

BACKGROUND

This section will introduce the key concepts necessary to understand the rest of this chapter. Digital forensic science and the Cloud computing model will be defined. Using these two definitions cloud forensics, a recently emerged branch of digital forensics science, will be presented.

Digital Forensics

Forensic science is the set of scientific methods for examining and gathering information about the past in order to support investigations. Digital forensics is a branch of this science and focuses on the identification and acquisition of digital evidence from electronic devices like laptops and smartphones as well as digital cameras and MP3 readers. It is defined digital evidence any "*information of probative value stored or transmitted in*